FIPS 140-2 Security Policy for Cisco Aironet AP1131AG, AP1232AG, and AP1242AG Wireless Access Points and BR1310G Wireless Bridge

This security policy contains these sections:

- Overview, page 2
- Physical Security Policy, page 3
- Roles, Services, and Authentication, page 6
- Secure Configuration, page 7
- Cryptographic Key Management, page 8
- Disallowed Security Functions, page 10
- Obtaining Documentation, page 10
- Documentation Feedback, page 11
- Cisco Product Security Overview, page 11
- Obtaining Technical Assistance, page 12
- Obtaining Additional Publications and Information, page 14

This document may be freely distributed.

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Overview

The Cisco Aironet AP1131AG, AP1232AG, AP1242AG, and BR1310G (collectively called *the modules*) are wireless access points that support the 802.11a/b/g wi-fi standards for communications, and 802.11i for security. It is a multiple-chip standalone cryptographic module, compliant with all requirements of FIPS 140-2 Level 2.

In the FIPS mode of operations, the modules support the Preshared Key (PSK) mode of authentication for network communications and uses the following cryptographic algorithm implementations:

- AES
- AES-CCM
- SHA-1
- HMAC SHA-1
- X9.31 Random Number Generator

This document details the security policy for the AP1131AG, AP1232AG, AP1242AG, and BR1310G cryptographic modules.

The evaluated platforms are summarized in Table 1.

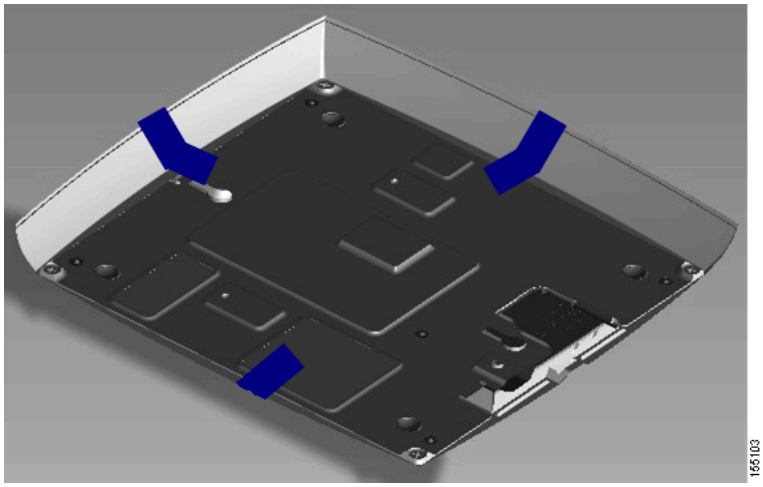
Table 1 Evaluated Platforms

Model	Firmware Version	Hardware Revision
AP1131AG	IOS 12.3(8)JA	C0
AP1232AG	IOS 12.3(8)JA	A0
AP1242AG	IOS 12.3(8)JA	A0
BR1310G	IOS 12.3(8)JA	C0

Physical Security Policy

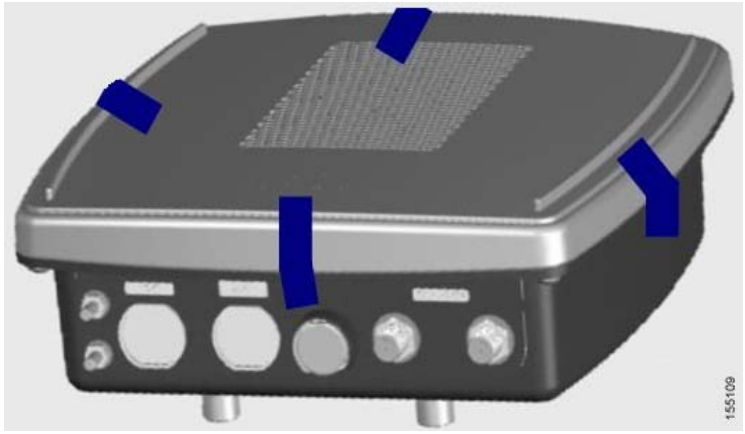
For the AP1131AG, place tamper evident labels over the bottom panel and over the top cover as shown in Figure 1.

Figure 1 Placement of Tamper-evident Labels for the AP1131AG



For the BR1310G, place tamper evident labels over the bottom panel and over the top cover as shown in Figure 2.

Figure 2 Placement of Tamper-evident Seals



For the AP1232G, put tamper evident labels over the reset button and over the bottom panel on each of the screws, over the panel on the bottom of the module as shown in Figure 3, and over the radio connected to the back of the module as shown in Figure 4. Note that a cap is placed over the reset button in order to prevent it from being pressed. The tamper evident label can be punched so the cap protrudes through it (as pictured) or the cap can be placed entirely underneath the label.

Figure 3 Placement of Tamper-evident Labels on the AP1232AG (front view)

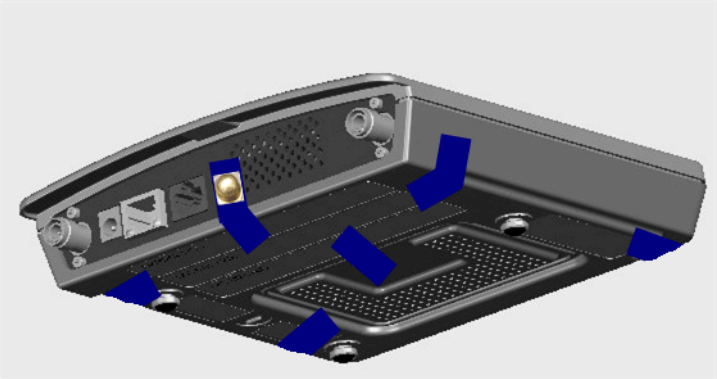


Figure 4 Placement of Tamper-evident Labels on the AP1232AG (rear view)

For the AP1242AG, put tamper evident labels over the removable top cover and the mode button as shown in Figure 6 and Figure 7.

Figure 5 Placement of Tamper-evident Labels for the AP1242AG (Underside of Cover)

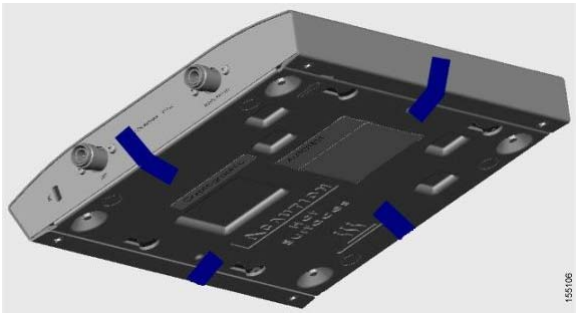


Figure 6 Placement of Tamper-evident Labels for the AP1242AG (Front View)

Roles, Services, and Authentication

This section describes the roles, services, and authentication types in the security policy.

Roles

The modules support operator access through the local console port. Remote access is not permitted. The modules support role-based authentication of Users and Crypto Officers, which are the only roles supported by the modules. Only one Crypto Officers password can exist.

Services

All services can be viewed by typing **?** from within the appropriate roles. This command shows all the services available to the role currently logged in.

The services provided are summarized in Table 2. Additional detail is provided in the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.

Table 2 Module Services

Service	Role	Purpose
Cryptographic Operations	User, Crypto Officer	Generate GMK and derive KCK, KEK, TK and GTK using the 802.11i protocol. Encryption and decryption of data in transit.
Self Test	User, Crypto Officer	Cryptographic algorithm tests, software integrity tests.
System Status	User, Crypto Officer	The LEDs show the network activity and overall operational status.
Key Management	Crypto Officer	Key and parameter entry, key output, key zeroization.
Module Configuration	Crypto Officer	Selection of non-cryptographic configuration settings.
Module Debugging	Crypto Officer	Crypto officers can review all system parameters and values for troubleshooting.

User Authentication

Passwords for all Users and Crypto Officers should be configured to include 8 or more characters, including both numbers and letters. The Configure Authentication Data section describes the commands to set up the passwords.

Secure Configuration

Configuration of the modules shall be performed only over a local link through the console connection. The Crypto Officer must ensure that the PC that is used for the Console connection is a stand-alone or a non-networked PC. Remote access is not permitted.

Follow these steps to prepare the secure configuration for the module:

1. Configure Authentication Data
2. Configure Ciphersuites for 802.11i
3. Configure Pre-Shared Keys for 802.11i
4. Disable Automatic Firmware Upgrades

Configure Authentication Data

The enable secret (the password for the Crypto Officer) must comprise 8 or more characters and must include both numbers and letters. Use these CLI commands to enable the password:

```
ap> enable
Password:
ap# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ap(config)# enable secret [PASSWORD]
```

Use these commands to set the user password:

```
ap> enable
Password:
ap# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ap(config)# username name password 0 password
```

The user password must contain 8 or more characters and must include both numbers and letters.

Configure Ciphersuites for 802.11i

The only 802.11i ciphersuite permitted is aes-ccm. This may be set using the following command syntax:

```
ap> enable
Password:
ap# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ap(config)# interface dot11Radio 0
ap(config-if)# encryption mode cipher aes-ccm
```

Configure Pre-Shared Keys for 802.11i

The only WPA2 mode permitted by this security policy is the Pre-shared Key (PSK) mode. Generation of pre-shared keys is outside the scope of this security policy, but they should be entered as 64-byte hexadecimal values with the following command syntax:

```
ap> enable
Password:
ap# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
ap(config)# interface dot11Radio 0
ap(config-if)# ssid samplessid
ap(config-if-ssid)# authentication open
ap(config-if-ssid)# authentication key-management wpa
ap(config-if-ssid)# wpa-psk hex 0 f42c6fc52df0ebef9ebb4b90b38a5f90
2e83fe1b135a70e23aed762e9710a12e
```

Disable Automatic Firmware Upgrades

The only firmware image permitted in approved mode of operations is Cisco IOS Release 12.3(8)JA. To disable automatic firmware upgrades, enter these commands:

```
ap> enable
Password:
ap# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ap(config)# no boot upgrade
```

In addition to disabling automatic firmware upgrades, the Crypto Officer is not permitted a manual upgrade of the module firmware.

Cryptographic Key Management

Cryptographic keys are stored in flash (for long term keys and security parameters) and in SDRAM (for active RSNAs (Robust Secure Network Association)).

The PSK (aka PMK) is electronically input into the module in plain text by the CO over a local console connection. The GMK is generated in the module using X9.31 FIPS approved PRNG. All other keys (KCK, KEK, TK & GTK) are derived using the 802.11i Key derivation protocol. The GTK is output to the client encrypted with the KEK.

Table 3 lists the cryptographic keys and CSPs used by the modules, and Table 4 lists the services that can access the keys and CSPs.

Table 3 Cryptographic Keys and CSPs

Name	Algorithm	Storage	Description and Zeroization
PRNG seed	X9.31	SDRAM	This is the seed for the X9.31 PRNG. It is updated by the X9.31 algorithm after the generation of every 8 byte block. The operator can reset the router to zeroize this CSP.
PRNG seed key	X9.31	SDRAM	This is the seed for X9.31 PRNG. It is updated periodically after the generation of 400 bytes; after this it is reseeded with router-derived entropy; hence, it is zeroized periodically. Also, the operator can reset the router to zeroize this CSP.

Table 3 Cryptographic Keys and CSPs (continued)

Name	Algorithm	Storage	Description and Zeroization
Enable secret	Shared secret	Flash	The obfuscated password of the CO role. However, the algorithm used to obfuscate this password is not FIPS approved. Therefore, this password is considered plain text for FIPS purposes. This password is zeroized by overwriting it with a new password.
User password	Shared secret	Flash	Role based authentication data for a user. This password is zeroized by overwriting it with a new password.
PSK (aka PMK)	Shared secret	Flash	The 802.11i preshared key (PSK). In the evaluated configuration, the PSK is used as the pairwise master key (PMK). It is zeroized by overwriting with a new value.
802.11i Key Confirmation Key (KCK)	HMAC- SHA-1	SDRAM	The KCK is used by IEEE 802.11i to provide data origin authenticity in the 4-Way Handshake and Group Key Handshake messages. Zeroized when the RSNA terminates
Key Encryption Key (KEK)	AES	SDRAM	The KEK is used by the EAPOL (Extensible Authentication Protocol over LAN) Key frames to provide confidentiality in the 4-Way Handshake and Group Key Handshake messages. Zeroized when the RSNA terminates.
Temporal key (TK)	AES-CCM	SDRAM	The TK, also known as the CCMP key, is the 802.11i session key for unicast communications. Zeroized when the RSNA terminates.
Group Master Key (GMK)	Random value	SDRAM	GMK is a precursor to the GTK i.e., GMK is used to derive GTK according to the 802.11i protocol.
Group Temporal Key (GTK)	AES-CCM	SDRAM	The GTK is the 802.11i session key for multicast communications.

Table 4 Key/CSP Access by Service

Role	Service	Key Access
User/Crypto Officer	Cryptographic Operations	• Generate GMK • Derive KCK, KEK, GTKand TK according to the 802.11i protocol.
	Self Test and Initialization	• Zeroize KCK, KEK, and TK • Initialize PRNG Seed
	System Status	• None

Table 4 Key/CSP Access by Service (continued)

Role	Service	Key Access
Crypto Officer	Key Management	• Read/Write PSK
	Module Configuration	• Read/Write User and Crypto Officer Passwords
	Module Debugging	• Read all module parameters

Disallowed Security Functions

These cryptographic algorithms are not approved and may not be used in FIPS mode of operations:

- RC4
- MD5
- HMAC MD5
- RSA

Self Tests

The following self tests are performed by the module:

- Firmware integrity test
- Power on self test of AES, AES-CCM, SHA-1, HMAC SHA-1 and X9.31 RNG algorithms
- Continuous random number generator test for Approved and non-Approved RNGs

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.
- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html